

ICO call for views on a direct marketing code of practice

The Information Commissioner is calling for views on a direct marketing code of practice.

The Data Protection Act 2018 requires the Commissioner to produce a code of practice that provides practical guidance and promotes good practice in regard to direct marketing.

While direct marketing is an important and useful tool to help organisations engage with people in order to grow their business or to publicise and gain support for their causes, it can also be intrusive and have a negative impact on people if done badly. This can cause reputational damage to organisations and, in some cases, result in fines or other regulatory action for breaking data protection laws.

So it is important that organisations ensure their marketing activities are compliant with data protection legislation (the General Data Protection Regulation and Data Protection Act 2018) and, where necessary, the Privacy and Electronic Communications Regulations 2003 (PECR).

We have previously published detailed direct marketing guidance. The new code will build on that guidance and address the aspects of the new legislation relevant to direct marketing such as transparency and lawful bases for processing, as well as covering the rules on electronic marketing (for example emails, text messages, phone calls) under PECR.

The European Union is in the process of replacing the current e-privacy law (and therefore PECR) with a new ePrivacy Regulation (ePR). However the new ePR is yet to be agreed and there is no certainty about what the final rules will be. Because of this we intend for the direct marketing code to only cover the current PECR rules until the ePR is agreed. Once the ePR is finalised and the UK position in relation to it is clear we will produce an updated version of the code which takes this into account as appropriate.

This call for views is the first stage of the consultation process. The Commissioner is seeking input from relevant stakeholders, including trade associations, data subjects and those representing the interests of data subjects. We will use the responses we receive to inform our work in developing the code.

You can email your response to directmarketingcode@ico.org.uk

Or print and post to:

Direct Marketing Code Call for Views
Engagement Department
Information Commissioner's Office

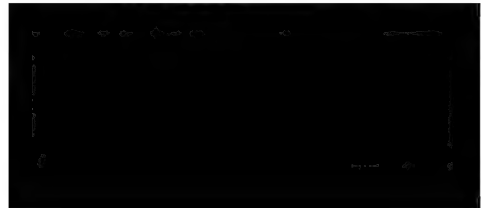
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the call for views, please email the [Direct Marketing Code team](#).

Please send us your views by 24 December 2018.

Privacy statement

For this call for views we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our [privacy notice](#).



Questions

Q1 The code will address the changes in data protection legislation and the implications for direct marketing. What changes to the data protection legislation do you think we should focus on in the direct marketing code?

No changes required per se – just clarification that PECR and GDPR can co-exist, the former representing the provision for direct marketing activity, the latter, the responsibilities for how a business manages data (in DM activity or other activity).

Q2 Apart from the recent changes to data protection legislation are there other developments that are having an impact on your organisation's direct marketing practices that you think we should address in the code?

☐ Yes

☒ No

Q3 If yes please specify

Q4 We are planning to produce the code before the draft ePrivacy Regulation (ePR) is agreed. We will then produce a revised code once the ePR becomes law. Do you agree with this approach?

☒ Yes

☐ No

Q5 If no please explain why you disagree

Q6 Is the content of the ICO's existing direct marketing guidance relevant to the marketing that your organisation is involved in?

☐ Yes

☒ No

Q7 If no what additional areas would you like to see covered?

There are 2 elephants in the room regarding existing guidance and indeed, the existing content on the following subjects are weak. One surmises the reason for weak guidance is that (with significant impact in certain industries) it is contentious to release new guidance and easier to simply wait until enforcement and penalties cascade through from other legal or regulator bodies in other areas of the EU – i.e. a cage the ICO would prefer not to rattle.

1. Weak content concerning 'Legitimate Interest' (LI) as affects Direct Marketing
2. Weak content concerning consent and general web-browsing processes, ad-tech and mar-tech

Regarding LI, the guidance should more clearly articulate that a balancing test is a mandatory part of an LI Assessment (LIA) and it is critical this balancing test is conducted with integrity. Say things like – 'if, for example 7 questions from a 14 deck of questions were answered positively as part of a balancing test, then a business should normally be able to evidence the necessary legal basis is established. As this falls to zero, any argument becomes more difficult, with scores of 5-6 representing a 'a good argument required' scores of 3-4 representing 'unlikely' and a score of 1-2 'almost impossible' to establish LI as a legal basis. It is in everyone's interests that LI continues as a valid legal basis of processing, including an allowance for subjectivity. Those businesses who pay little or no heed to the integrity of an LIA mean it will regrettably be necessary for a replacement to this legal basis – a replacement which is only likely to be more binary and less flexible with genuine scenarios where data processing is required.

Evidencing a genuine forensic of consent is critical before a business might use a data record for its own purpose. Outside of questions a firm may have in connection with its consent tag for its own records (e.g. records on its own CRM system), a businesses 'go to' solutions for supply of new records are either list brokers or ad-tech/social media ad 'data-launderers', the latter it seems no-one pretends to understand. In both cases, regulators are defining the actual rules on using this type of data through investigation outcomes – for list brokers; the EDML, Boost Finance and Emma's diary cases and in ad-tech/social media ad space, the Bavarian LDA,

CNIL/Vectuary case as well as the ECJ case with Wirtschaftsakademie Schleswig-Holstein. What is clear here is that the original source data subject has a right to be protected from the acquisition of their personal data without GDPR level consent. Period. And yet, brokers of all manner and operating in all channels persist with trade bodies including the DMA for Direct Marketing and the IAB for Digital Marketing continue with incorrect advice and consent frameworks for it's members....yet the advice they give is incorrect.

Urgent update to guidance on these issues is required.

Q8 Is it easy to find information in our existing direct marketing guidance?

☒ Yes

☐ No

Q9 If no, do you have any suggestions on how we should structure the direct marketing code?

ico.
Information Commissioner's Office

Q10 Please provide details of any case studies or marketing scenarios that you would like to see included in the direct marketing code.

In addition to clarification of those issues raised in answer 7, there is also clarification required in respect of an employee's general web-browsing processing.

Please answer (my phone number is [REDACTED] or my email is [REDACTED]) whether web-browsing is within the scope of GDPR, particularly;

- a) when sites browsed to contain personal data
- b) when the default setting of a browser is that it builds a list through default functionality – i.e. the browser history

Even in a corporate scenario (where one would expect policies including a data protection policy and if appropriate, BYOD), does the corporate have an obligation to actively control (and document) an end-user's internet browsing activity.... To conduct bespoke risk assessment, determine

retention, document use and all of the steps required of an audit when the scope of the data is more clearly determined as belonging to the corporate body.

Should this be the case – i.e. the ICO determines browsed-data is within the scope of regulation....ergo personal data processing is taking place, then is it then required of the organisation to put in place encryption or other data minimisation processes to reduce risks to those data subjects?

I have an combined encryption and pseudonymisation process in mind which achieves this risk reduction and am hopeful to access your sandbox next year to see this through. Any earlier interpretation of what I am doing here would be very gratefully received. Please note, the encryption/pseudonymisation process does not anonymise the record to necessary GDPR standard as we need to un-encrypt (what will be a url) later in our processes – i.e. to take a user back to the original web-page displayed. I'm just incredibly interested in your interpretation on this initiative and its raison d'être in minimising breach risk.

Q11 Do you have any other suggestions for the direct marketing code?

About you

Q12 Are you answering these questions as?

☐

☐

☐

☐

☐

☐

☒

- A public sector worker
- A private sector worker
- A third or voluntary sector worker
- A member of the public
- A data subject
- An ICO employee
- Other

If you answered 'other' please specify:

Start up technology company

ico.
Information Commissioner's Office

Q13 Please provide the name of the organisation that you are representing.

Guru Jamez Ltd

Q14 We may want to contact you about some of the points you have raised.
If you are happy for us to do this please provide your email address:

[Redacted]

Thank you for taking the time to share your views and experience.

